WHITE PAPER

Toward A Next Generation Strategy:

Learning From Katrina And Taking Advantage Of New Technologies

Dale Hatfield
University of Colorado
Interdisciplinary Telecommunications Program

Phil Weiser
University of Colorado School of Law and
Interdisciplinary Telecommunications Program

EXECUTIVE SUMMARY

In the aftermath of Hurricane Katrina, it appears that a unitary reliance on Land Mobile Radio systems (LMRs) failed public safety agencies, leaving them without any source of communications once their transmission towers went down. Notably, the failure of these agencies—and policymakers more generally—to take advantage of recent technological developments to design a more robust communications system proved to be the Achilles' heel of responding effectively in the wake of a disaster.

As we explain in this White Paper, there is a next generation *architecture* for public safety communications that would bring together existing LMRs, commercial terrestrial services, satellite technology, and wireless broadband systems to provide a robust, reliable, secure, and interoperable broadband communications system. Significantly, the technology exists to make such an architecture a reality; the challenge for policymakers is to provide the leadership to make this important development a reality. To advance this vision, policymakers should ensure that (1) satellite and terrestrial providers are afforded the opportunity—through pro-market and innovative spectrum policies—to develop effective offerings for public safety agencies; and (2) important financial support for public safety agencies promotes this type of a hybrid, next generation architecture.

"[I]n the long term, we will need to learn from this event and work together to improve the reliability, survivability, and security of our nation's telecommunications networks."

Joint Statement of Chairman Kevin J. Martin and Commissioner Michael J. Copps Following Their Visit to the Gulf State Region Affected By Hurricane Katrina **(September 9, 2005).**

I. Introduction

In light of the events and tragic aftermath of Hurricane Katrina, we have revised our earlier White Paper, "Taking A Fresh Look At Public Safety's Spectrum Needs: Toward A Next Generation Strategy for Public Safety Communications" (prepared on behalf of Mobile Satellite Ventures LP (MSV)[1]) to explain how policymakers should respond to rising concerns about breakdowns in public safety communications systems. In assessing the communication breakdowns that appear to have taken place in the wake of Katrina, we observed just the failings noted in our earlier paper—i.e., the relevant public safety agencies lacked interoperable, redundant, secure, and economic methods of communicating with one another. Unfortunately, in the wake of this tragedy, many have advocated the traditionally recommended prescriptions for improving public safety communications (i.e., more dedicated spectrum and more money for upgraded Land Mobile Radio Systems (LMRs)). As we explain, however, both the needs underscored by Katrina and the capabilities made possible by modern technology suggest a next generation strategy of a *flexible architecture* that can incorporate traditional LMRs along with satellite, terrestrial, and wireless broadband systems.

The flexible architecture we embrace is one that will almost certainly be available before the completion of the digital transition and the availability of more spectrum for public safety agencies. In particular, the concept of "multi-mode" radios is already a widespread reality in most segments of the marketplace (except for public safety).[2] Such multi-mode radios will be even more robust once the recently authorized **"ancillary terrestrial component"** (ATC) of mobile satellite services provides becomes an option for public safety agencies. Even using

[1] MSV is the entity authorized by the Federal Communications Commission in 1989 to construct, launch, and operate a Mobile Satellite Service system in the L-band. MSV's licensed satellite (AMSC-1) was launched in 1995, and MSV began offering service in 1996. MSV is also the successor to TMI Communications and Company, Limited Partnership (TMI) with respect to TMI's provision of L-band MSS in the United States. Today, MSV offers a full range of land, maritime, and aeronautical satellite services, including voice and data, using both its own U.S.-licensed satellite and the Canadian-licensed L-band satellite licensed to Mobile Satellite Ventures (Canada) Inc. In November 2004, the Federal Communications Commission authorized MSV to supplement its satellite service with ATC. See Mobile Satellite Ventures Subsidiary LLC, Order and Authorization, DA 04-3553 (Chief, International Bureau, November 8, 2004).

[2] *See, e.g.,* Mike Dano, *LG, Qualcomm Release Dual-Mode Technology,* RCR Wireless News (September 23, 2005) (www.rcrnews.com/printwindow.cms?newsId=24251&pageType=news) (discussing latest multi-mode technological developments).

traditional satellite technology, firms like MSV are able to provide service to a number of public safety agencies today. But beginning within the next couple of years, after completing the deployment of an ATC service, MSV (and perhaps others) will be able to expand this service and offer it more efficiently to public safety agencies across the United States and provide it as a critical part of a realistic and effective nationwide interoperable broadband mobile communications system for public safety agencies. Such a convergence between wireless and satellite is already becoming a reality in other countries, such as South Korea, meaning that its prospects in the United States will depend on whether the market appreciates the benefits of a built-in satellite backup, not on whether the product is technically feasible.[3]

This White Paper proceeds in four parts. First, we review the events around Hurricane Katrina and underscore how public safety communications systems failed to operate effectively. Second, we outline the requirements for an ideal public safety network, noting the often cited shortcomings of traditional commercial providers. Third, we explain how public safety agencies can utilize networks provided by commercial providers—particularly hybrid satellite and terrestrial systems—to satisfy the relevant requirements in a cost-effective fashion. Finally, we explain how policymakers can facilitate the transition to such optimal hybrid networks.

I. Katrina and Its Lessons

The aftermath of Hurricane Katrina, when many mission critical networks were down and unavailable to key governmental officials and first responders, made clear that effective communication during a crisis should not and cannot be a luxury. In particular, if mission critical networks do not live up to their name—i.e., are not reliable, survivable, and secure—first responders will be left unable to perform their job effectively. In the case of Katrina, public safety agencies realized that traditional Land Mobile Radio Systems (LMRs)—even along with commercial wireless systems—are unlikely to remain widely available under certain adverse conditions. As Federal Communications Commission (FCC) Chairman Martin emphasized, "[i]f we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications."[4]

[3] Katrina Could Unite Wireless, Satellite Industries, Communications Daily (September 22, 2005).

[4] Statement of Kevin J. Martin, Hearing on Communications in A Disaster 7 (September 22, 2005).

As many accounts have reported, Hurricane Katrina left Louisiana's governmental communications systems in shambles. Governor Kathleen Blanco reported early on that wireless networks throughout the state were down and that many state officials were cut off from communicating with one another. As Reuters put it, "[t]he collapse of the communications network in the New Orleans area has been widely blamed for contributing to the disaster there, as local officials were unable to talk to each other and to federal authorities to arrange relief in the days after Katrina laid waste to the city."[5]

Based on preliminary reports, it appears that failed communications networks emerged as an Achilles' heel of first responder efforts whereas a bright spot was the use of satellite units that remained effective throughout the tragedy. Keith Sims, the telecom chief of Tampa Electric who brought a team to New Orleans to help repair the damage, explained that "[c]ellphones don't do much good after a hurricane" whereas satellite units worked very well in the storm's aftermath. As another user of satellite technology put it, "it's the only way [our employees] can talk to one another."[6] Noting that satellite systems remained intact during the crisis, FCC Chairman Martin explained that they "helped to bridge the gaps left by outages by providing satellite phones and video links to law enforcement, medical personnel, emergency relief personnel, and news outlets."[7] In sum, as one trade publication explained, "[a]fter Hurricane Katrina wreaked havoc on the Gulf Coast terrestrial wireless network, satellite phones and satellite data services played a critical role in filling communication gaps left by the storm."[8]

---

[5] Wireless Carriers Reconnect in New Orleans, CNET News.com (September 4, 2005) (http://news.com.com/Wireless+carriers+reconnect+in+New+Orleans/2100-1039_3-5849066.html); *see also* Mimi Hall, *Hard Lessons of Katrina Being Put to Immediate Use, USA Today* 1A (September 22, 2005) ("When Katrina wiped out communications along the Gulf Coast, officials and key emergency workers were cut off from each other. That contributed greatly to the chaos on the ground.").

[6] Paul Davidson, Satellite phones provide critical link to outside world, *USA Today* (September 5, 2005) (http://www.usatoday.com/tech/wireless/2005-09-05-satellite-phones_x.htm?POE=TECISVA); see also Press Release, State Wildlife Agency Playing Large Role in Hurricane Relief (September 6, 2005) (http://www.mdwfp.com/Level1/NewsRoom.asp?ID=302) (explaining that satellite units provided a critical means of communicating with one another, enabling different relief efforts to work together).

[7] *See, e.g.,* Statement of Kevin J. Martin, Hearing on Communications in A Disaster 3 (September 22, 2005).

[8] Katrina Could Unite Wireless, Satellite Industries, COMMUNICATIONS DAILY (September 22, 2005).

Along with other providers of mobile satellite services, MSV offered crucial assistance to governmental organizations in the affected area. As MSV CEO Alex Good related to FCC Chairman Martin, many satellite terminals were being used to provide access to reliable, quality communications for agencies ranging from the American Red Cross, the Federal Emergency Management Agency to the Louisiana Department of Homeland Security. Even with MSV providing access to these terminals at cost and providing free airtime to state and local public safety agencies in the affected area, the economics of such devices do not lend themselves to widespread use (i.e., terminals costing thousands of dollars and air time in the several dollar a minute range)—thus leaving many first responders cut off from crucial communications.

Based on currently available information, a central lesson underscored by Katrina is that relying solely on Land Mobile Radios (LMRs) does not provide the reliability and survivability sometimes suggested by its boosters. In particular, some have claimed that governmental systems that are maintained by public safety agencies and protected in ways that commercial networks are not would be sufficiently robust to continue operating during an emergency. Such claims, however, generally focus on a particular threat—traffic from ordinary users overwhelming the network. Other claims about commercial systems—say, the need to provide backup power, enable re-charging of the handsets, and the lack of coverage in some areas—may prove problematic in certain cases. Nonetheless, an optimally designed system (i.e., a flexible one allowing the use of satellite technology and multiple networks) can provide the greatest assurance that public safety communications will remain available during a time of crisis.

In short, it is essential that mission critical networks be able to survive natural or manmade disasters so that first responders can perform their role effectively. Katrina reminds us that LMR systems can be destroyed even when protected by some measures not used by their commercial brethren, underscoring that the best assurance of survivability is the use of a flexible system that includes satellite technology. As we discuss in Part II, the flexibility and redundancy of system that includes satellite technology is one only of a number of requirements that we believe are important for a next generation public safety communications system.

II. Requirements For A Next Generation Public Safety Communications System

In the wake of 9/11 and Katrina, combined with an emerging awareness of the shortcomings of current public safety communications networks, most policymakers are familiar with the arguments for developing a next generation (i.e., broadband and interoperable) mobile radio network. Thus, rather than focus on the particular applications and rationale for such a network, this Part explains the key requirements of any such network. In particular, we explain the need for (A) ubiquitous access; (B) reliability; (C) interoperability; (D) configurability; and (E) security. In so doing, we make a special effort to acknowledge the criticisms traditionally leveled at commercial wireless providers.

A. Ubiquitous Access

A fundamental requirement for public safety mobile radio networks is that they must function in all areas served by first responders. The need for ubiquitous access is a notorious shortcoming of modern commercial mobile radio networks, which often do not serve more remote areas.[9] As commercial providers underscore, the territory they do serve often includes 90% of the population. Because of the increasingly urbanized nature of the nation, however, this coverage can be achieved while covering less than 10% percent of the U.S. land area. Given this limited geographic reach and the lack of coverage for the other 10% of the population, public safety agencies traditionally have eschewed reliance on commercial systems and have developed their own land mobile radio (LMR) systems. Significantly, even many LMR systems operated by public safety agencies do not cover their entire territory. The New Mexico State Police's system, for example, cannot reach 15% of the state—and is limited to voice communications.[10]

The second aspect of ubiquitous coverage involves ensuring service in buildings. Historically, the lack of radio communications ability within buildings represented a notable failing of public safety LMRs—and one that has led to tragic results during emergency situations such as 9/11.[11]

---

[9] Mary Greczyn, *FCC Weighs Whether To Scrap 20-Year-Old Cellular Mandates,* COMMUNICATIONS DAILY (August 7, 2002) (reporting that digital cellular networks reached only around 50% of the population).

[10] James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf).

[11] *Increasing FDNY's Preparedness*, August 19, 2002 (www.nyc.gov/html/fdny/html/mck_report/toc.html).

To respond to this failing, some cities have required in-building coverage plans as part of any new construction (such as the installation of bi-directional amplifiers). In-building systems can be expensive, however, with major high rise buildings requiring an investment of $1-$2 million.[12]

B. Reliability

For public safety agencies, the second critical requirement is that "mission critical" networks be able to survive and continue to operate during natural or man-made disasters, such as hurricanes, earthquakes, fires, or a high-powered blast caused by a bomb. In many cases, traditional commercial networks are not engineered to withstand such disasters—either because they are not protected or because they do not have sufficient generation capacity or battery back-up to stay online if the power grid goes down. Moreover, even if available, commercial systems are often overloaded by calls during emergencies; as one report explained, "[e]xperience has shown that such systems are often the most unreliable during critical incidents when public demand overwhelms the system."[13] Tragically, as Katrina reminds us, disasters can destroy all available terrestrial systems, meaning that the only way to assure reliability and available access is to incorporate a satellite component. In short, through some combination of public or commercial wireless and satellite systems, it is clear that public safety agencies need access to a system that will remain operational and available during emergencies and that will afford them with priority access.

C. Interoperability

As numerous policy observers and policymakers have emphasized, the lack of interoperability among public safety agencies remains a grave concern.[14] As the Federal Communications Commission has defined the issue, interoperability is "[a]n essential communications link within public safety and public service wireless communications systems which permits units from two or

---

[12] Public Safety Wireless Network Program, *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report* (November 2002) (http://www.safecomprogram.gov/NR/rdonlyres/2311FAAD-18DE-4EA9-BC5A-6C99CC24BAFA/0/In_Building_In_Tunnel_Ordinances_Report.pdf).

[13] National Task Force on Interoperability, *When They Can't Talk, Lives Are Lost* (February 2003) (http://www.agileprogram.org/ntfi/ntfi_brochure.pdf).

[14] *See, e.g.,* Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 24 (April 2005) (http://www.gao.gov/new.items/d05380.pdf) ("The lack of communications interoperability among firefighting and other first-responder agencies can impair their ability to respond to emergencies quickly and safely, and cost lives among responders and those they are trying to assist.").

more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results."[15] Stated more simply, interoperability means that two (or more) emergency service providers—say, a paramedic and a fire fighter—can communicate with one another in an efficient, reliable, and secure fashion. Given the American system of government, with thousands of local agencies that enjoy local autonomy, it should not be surprising that different jurisdictions (as well as, unfortunately, agencies within the same jurisdiction) have often made decisions that inadvertently do not promote this goal.

In looking back at the numerous inquiries into the causes of the continuing lack of interoperability, several themes emerge as predominant. First, many jurisdictions lack the funds to upgrade their systems (some often 20-40 years old) and, more fundamentally, are unable to plan effectively for their wireless communications needs. Second, local public safety administrators (either managers like the Chief of Police or the relevant IT professional working in an agency) are often attached to their current approaches and unwilling to give up control to facilitate a greater sharing of resources and technology—an understandable concern where they are responsible for ensuring that communications systems work effectively. In this respect, achieving interoperability is not simply a matter of upgrading equipment, but also of changing the culture of operating in isolation and without full regard for how other public safety agencies operate. To be sure, there are some notable successful ventures that have galvanized regional cooperation between different agencies, such as the Capital Wireless Integrated Network (CapWIN) project that has brought together over 40 local, state, and federal public safety agencies in the Washington, D.C. metro area into a system that provides important real-time communication abilities and access to government databases. Such projects, however, require a system of effective governance involving a number of discrete agencies willing to coordinate their radio equipment needs. Notably, as many other failed initiatives demonstrate, ambitious visions of developing a single system to be used by all relevant agencies are very difficult to achieve and thus more flexible approaches are far more likely to be successful.[16]

---

[15] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 ¶ 76 (1998).

[16] National Task Force on Interoperability, *Why Can't We Talk: Working Together to Bridge The Communications Gap to Save Lives, Supplemental Resources* 19-22 (February 2003) (http://www.agileprogram.org/ntfi/ntfi_supplemental.pdf) (detailing Colorado's failed approach).

A third major cause of limited interoperability is that many agencies cannot communicate with one another because they use equipment with incompatible (and often proprietary) technology. In some cases, these sorts of challenges can be addressed by developing intermediary patches—i.e., a dispatch center (using "bridge equipment") that can interconnect different systems—but such "second best" solutions are expensive and inefficient compared to more rationally designed systems.

Although none have taken hold completely, there are a number of efforts that have attempted to overcome the lack of common standards and to develop ones to facilitate interoperable public safety communications. Notably, the APCO-sponsored Project 25 standard and the European-developed TETRA standard have both sought to advance this goal; more recently, the international "Project MESA" initiative has begun to develop a next generation standard. As for the exchange of data, a coalition of first responders is now working to develop an Extensible Markup Language (XML)-based standard (i.e., the Emergency Data Exchange Language (EDXL)) to enable the panoply of different agencies that might be called to the scene of an accident (i.e., public safety, transportation, and medical personnel) to share information with one another[17] In its effort to facilitate interoperability, the Federal Communications Commission chartered an advisory committee (the Public Safety National Coordination Committee) that has recommended technical and operational standards for spectrum that will be made available to public safety agencies.[18] Finally, the Department of Homeland Security's SAFECOM initiative has developed a "statement of requirements" that, in the words of SAFECOM's Director, provide an "architectural framework for future interoperable public safety communications."[19]

The final cause of limited interoperability is that local public safety agencies often lack access to (or may not choose to use) radio spectrum in the same frequency bands used by sister

[17] Diane Frank, *First Responders Seek Common Lingo*, FEDERAL COMPUTER WEEK (March 15, 2004) (http://www.fcw.com/article84556).

[18] *See The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, Fifth Memorandum Opinion and Order, __ FCC Rcd __ (2005) (considering recommendations).

[19] Press Release, Homeland Security First to Define Interoperability Requirements for Nation's First Responder Community (April 26, 2004) (http://www.dhs.gov/dhspublic/display?content=3513).

agencies. As a result, public safety agencies—which use any one of ten different bands of spectrum—often cannot communicate with one another even when using compatible technology. To rectify this situation, many in the public safety community have suggested that the transition to digital television, which will open up 24 MHz of spectrum in the valuable 700 MHz band for public safety uses,[20] should alleviate such concerns. But, to understate matters, it remains "somewhat elusive" whether the transition will be completed by 2006—or even 2009, for that matter—and "no public safety agency can logically budget for equipment that uses radio spectrum that is not yet available for them."[21]

In evaluating the spectrum issue, it is important to make clear that this aspect of interoperability might be unsolvable because different agencies often have good reasons for choosing different bands. In short, there are big differences in propagation characteristics between the lowest frequency band and the higher frequency bands used by public safety agencies; consequently, agencies in, say, mountainous areas have compelling reasons for choosing different bands than those agencies in very different (and possibly adjacent) areas. Thus, even if the FCC could identify adequate available capacity, it would still be unwise to force all public safety agencies into a single band.

D. Configurability and Flexibility

The ability of public safety networks to provide one-to-many communications (think "calling all cars") is essential to their effectiveness. Moreover, it is important that such networks be flexible and configurable so that they can include other groups (say, utilities when damage to an electric grid is involved) on an as-needed basis. In some cases, both of these features—i.e., a one-to-many functionality and an ability to create ad hoc networks of users—were lacking in traditional commercial networks. Increasingly, however, modern commercial networks (which are often software-based and designed for multiple applications) can support applications specialized for first responders, including sophisticated push-to-talk features.

---

[20] *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 (1998); *Reallocation of Television Channels 60-69, the 746-806 MHz Band*, Report and Order, 12 FCC Rcd 22,953 (1997); Balanced Budget Act of 1997, Pub. L. No. 105-33, § 3004, 111 Stat. 251 (1997) (codified at 47 U.S.C. § 337(a)(1)).

[21] *Why Can't We Talk,* supra, at 53.

E. Security

For public safety agencies, protecting the privacy of communications and guarding against malicious attacks on their communications services are critical priorities. To keep information private and guard against attacks, secure communications systems must encrypt communications (so that unauthorized users are not able to intercept them) and bilaterally authenticate both remote users and servers (to limit who has access to the system). In an ideal system, encryption keys can be dynamically assigned from a central management system so that additional users can be added as needed. Again, traditional commercial networks tend to lack sophisticated encryption and authentication capabilities. Going forward, commercial systems, such as the system MSV is developing for its ATC network, will increasingly deploy more sophisticated security features—such as Public Key Infrastructure (PKI)—and allow for applications that can provide additional security (e.g., through the use of stronger encryption, such as NSA Type-1).

III. MSV's Existing Satellite and Future ATC Services Provide Important Benefits to Public Safety Agencies

In evaluating the communication needs of public safety agencies, policymakers should reject the calls for a "one-size fits all" solution and recognize, as the Federal Wireless Policy Committee has put it, that "more than one service may be required to support" a next generation public safety network.[22] In particular, policymakers should promote a hybrid approach that would incorporate LMR systems along with terrestrial, satellite, and emerging wireless broadband systems. Such solutions are only beginning to be tested, but it is increasingly apparent that traditional LMR systems can be provided along with ancillary terrestrial component satellite handsets that automatically switch between cellular and satellite systems (depending on which is available). Moreover, by designing such systems in a modular fashion, they can rely on

[22] Federal Wireless Policy Committee, *Federal Functional Requirements for Commercial Wireless Services* (Dec. 11, 2001) (http://www.fwuf.gov/docs/rev_dec01.pdf); *see also* James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders,* FRONTLINE FIRST RESPONDER (June 2003) (http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf) (highlighting virtues of a multi-mode solution); Michael McShea & Richard Davis, *A Hybrid Approach*, MISSION CRITICAL COMMUNICATIONS 57 (April 2005); Alan Shark, *Don't Rule Out Either Option*, MISSION CRITICAL COMMUNICATIONS 60 (April 2005) ("no one system can or should meet all jurisdictional mission-critical needs").

wireless broadband networks, such as those using WiFi technology as well as still emerging technologies (like the next generation WiMAX standard). Notably, a WiFi-like system, like satellite technology itself, is relatively robust and, as demonstrated in the aftermath of Katrina, can be important in assisting the communications needs of public safety agencies.[23]

One important reason for relying on commercial systems in general and hybrid satellite-terrestrial systems in particular is that they enable public safety agencies to benefit from the considerable economies of scale and enhanced functionalities that commercial providers can offer. Even under the very best of circumstances, public safety agencies are generally not able to build up the economies of scale and develop the network efficiencies of their commercial brethren. (This explains, in considerable part, why public safety equipment is generally quite expensive.) At a minimum, then, public safety agencies should take advantage of the favorable economics of commercial systems and expand their use of "off the shelf" services and products for at least some of their communications needs. As we explain below, MSV's satellite services in general and its hybrid satellite-terrestrial offering in particular meet the requirements outlined above and are well suited to be a valuable component of public safety wireless systems.[24]

To supplement traditional terrestrial networks, it is critical to incorporate satellite services into public safety wireless systems. First, as Katrina made clear, satellite systems are the best means of ensuring that public safety communication systems remain operational during dire circumstances. Second, as the case of the New Mexico State Police demonstrates, satellite technology can assure complete coverage to public safety agencies. In particular, the New Mexico State Police Department has compensated for the lack of ubiquitous coverage and ability to carry data on its private LMR by contracting with MSV for access to a satellite-based solution that provides ubiquitous coverage, reliable push-to-talk services, and access to data communications capabilities.

---

[23] Kenneth Moran, Presentation at the Agenda Meeting of the Federal Communications Commission (September 15, 2005); *see also* Clive Thompson, Talking In The Dark, N.Y. Times Magazine 24 (September 18, 2005) (discussing how Wi-Fi-like systems using mesh technology can provide reliance and redundant communication networks).

[24] MSV is the leading developer of ATC systems, with 800 different covered claims in its 6 patents received to date and 70 additional patents pending. *See* Press Release, Sixth Comprehensive Patent Issued to Mobile Satellite Ventures (May 18, 2005) (http://www.msvlp.com/pr/news_releases_view.cfm?id=62).

Finally, with the FCC approved ATC architecture that MSV will begin rolling out for its hybrid satellite-terrestrial system, the price of the service will be substantially less than current satellite systems. By using mainstream devices as well as more efficient terrestrial systems where appropriate, a hybrid satellite-terrestial system provides significant cost savings *vis-à-vis* traditional satellite systems and will be available at reasonable prices from the launch of the product. More fundamentally, by using a terrestrial component, such systems can build up significant economies of scale that drive down the overall cost of the relevant equipment, meaning that the price of this service will decline dramatically as subscribers adopt it and the network enjoys greater scale economies. Significantly, even as to one of the advertised strengths of private LMR systems *vis-à-vis* commercial networks—the ability to provide coverage wherever it is needed—hybrid satellite-terrestrial systems can provide the best of both the commercial model as well as the traditional LMR systems. Thus, for carriers looking at the expense of adopting new LMR systems for remote areas and the ongoing costs of maintaining the necessary equipment, a hybrid satellite-terrestrial system provides an exciting alternative.

MSV's network provides a reliable and flexible wireless communications product that will become even more attractive once its ATC service is deployed. Unlike most commercial networks, hybrid satellite-terrestrial systems can be used when the local power grid fails or, in a situation like Katrina, when the available terrestrial networks are inoperable. In particular, hybrid satellite-terrestrial handsets can switch seamlessly and instantaneously between cellular networks (when a base station is operating nearby) and a satellite network (when there are no base stations in the area). In terms of providing priority access, MSV is designing its system so that, in the case of emergency events, the public safety operators can enjoy priority access to the extent necessary to preserve public safety communications. To do so, MSV is incorporating priority-precedence features contained within today's 3 G (and some 2 G) cellular standards.[25] Moreover, with its satellite network, MSV can provide superior call completion rates—even for calls that require coast-to-coast connectivity—when delivering "on network" calls that eliminate (or, in some cases, limit) any dependency on the external wireline network.

[25] The essence of priority and precedence features contained in, or under development for, 3G cellular standards, is that they enable pre-defined user classes to obtain priority access to wireless communications resources. Consider, for example, the enhanced Multi-Level Precedence and Preemption (eMLPP) feature within the Global System for Mobile Communications (GSM) air-interface, which provides for up to five distinct priority classes that (during periods of congestion) allow an "emergency call" to queue for the next available radio channel.

In terms of flexibility and configurability, MSV's hybrid satellite-terrestrial system will allow for the creation of ad hoc user groups of 2 to 10,000 that can use push-to-talk functionality and communicate among an interdisciplinary team through a large group dispatch service. Significantly, MSV expects the set-up time for such push-to-talk functionality to be similar to its existing offering, with a range of 1.5-2.0 seconds for talk group initiation and a delay between speakers of about 0.5-0.75 seconds. To be sure, this system may not be appropriate for "shoot-don't-shoot" situations, but should be adequate for an array of scenarios where push-to-talk systems are used by public safety agencies, including nearly all of the first responder communications needs in the wake of Katrina.

Increasing their reliance on commercial systems such as MSV's hybrid satellite-terrestrial system does not mean that public safety agencies should abandon their existing LMR systems. Rather, today's LMR systems often serve a very useful purpose and should be an important part of a hybrid network architecture. Along these very lines, both mission critical networks and critical infrastructure companies (such as utilities like the Tennessee Valley Authority) have begun to gravitate away from relying solely on their private networks. In particular, a number of entities that previously relied solely on their LMRs have concluded that they should continue to maintain such networks, but rather than upgrade them, they can increase productivity and cut costs by moving towards an integrated architecture that includes commercial wireless networks.

In terms of developing an optimal network architecture, public safety agencies should also be open to taking advantage of advances in wireless broadband technology developed for unlicensed spectrum. A public safety network might use, for example, current wireless local area network (WLAN) technology (i.e., the 802.11 (WiFi) standard) and, eventually, next generation systems (e.g., 802.16 (WiMAX) systems). To foster the adoption of such systems by local governments, the FCC recently made available access to spectrum in the 4.9 GHz band. As the FCC stated in its press release, "public safety licensees [can now] use a single, low-cost device to access the 4.9 GHz band, the U-NII band, and the ITS band, allowing them to enjoy savings that are typically limited to the high-volume commercial market."[26] Recognizing this opportunity, some police departments, like that of Salida, Colorado, have adopted solutions based

[26] News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (November 9, 2004) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254117A1.doc).

on this technology, saving money and making police officers more productive in the process.[27] One means of providing wireless broadband service is to use ad hoc mesh networking systems. At present, such systems are still in their early stages, but they promise (as one vendor put it) "infrastructure-free, automatically established and maintained, and agile" network architectures.[28] The promised effectiveness of such systems, which rely on a different architecture from today's established wireless technologies, reflects their ability to "forward data one hop at a time over a distributed network of autonomous nodes using new and more reliable and efficient schemes."[29] To limit the need for a widespread deployment of devices with the embedded ability to re-transmit communications (i.e., routers), some cities have deployed systems with transmitters placed on existing infrastructure (like streetlamps) and with intelligent access points to connect to wired infrastructure at particular points. In Garland, Texas, for example, the local law enforcement agency decided to rely on such a network, concluding (after an experimental use of the technology on a limited basis) that installing access points and wireless routers on existing infrastructure would be cheaper than building new transmission towers for either cellular or private LMR transmissions towers.[30] Finally, mesh networking systems, which rely on the basic Internet suite of protocols, can be secured by installing firewalls and other security protections.

In short, an optimal public safety architecture would use a flexible system to accommodate different technologies. As depicted in Figure 1, a public safety agency can use a multi-mode device to access a hierarchy of wireless networks, beginning with a public safety LMR system at the center, then a commercial terrestrial network such as MSV's ATC service and finally a satellite overlay.[31] As noted above, public safety agencies might also choose to integrate a

[27] Jim Renton, *Notebooks and Wi-fi Keep Colorado Cops on the Beat*, MOBILE COMPUTING NEWS (March 8, 2004) (http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html?track= NL-315&ad=477866&Offer=t3.8).

[28] Michael Rauf & Eric Lefebvre, *Keeping the Wireless Connection Running*, 9-1-1 MAGAZINE 58 (Jan/Feb 2003) (http://www.novaroam.com/downloads/nr_911article.pdf)

[29] Rick Merritt, *Darpa Looks Past Ethernet, IP Nets*, EE TIMES (April 26, 2004) (http://www.eet.com/showArticle.jhtml?articleID=19200111).

[30] Kris Middaugh, *No More Towers*, GOVERNMENT TECHNOLOGY (May 2004) (http://www.govtech.net/magazine/story.php?id=90189).

[31] Hybrid satellite-terrestrial systems rely on a satellite system that uses the same band of spectrum for an integrated terrestrial system. With such a system, MSV will achieve important spectrum efficiencies and economies of scale which will result in lower cost and more user-friendly consumer equipment than current MSS equipment. Such advancements are critical to deployment of MSV's next generation system and will redound to the benefit of public safety agencies that adopt it.

terrestrial wireless broadband network. In any event, the core design principle is that networks should be extensible to other terrestrial networks in addition to the core commercial terrestrial and satellite components.

Both commercial and public safety-driven considerations explain why multi-mode networks are increasingly practical and appropriate. Consider, for example, that today's ordinary consumer wireless devices have two to four bands and at least some of tomorrow's devices will use WiFi networks where available (not to mention a GPS receiver, Bluetooth functionality, and even a receiver for specialized TV broadcasts). With an extensible network, the keys to integrating them together are (1) facilitating the back-end integration of the commercial network and one or more LMR systems; and (2) gradually adding new user devices that incorporate satellite connectivity, including push-to-talk. In principle, this integration can be accomplished by incorporating a second chipset that would enable the device to use a satellite-adapted ersion of a mass-market air interface (MMI) such as GPRS, CDMA, OFDM or WiMAX.[32]

Based on current estimates, MSV believes that an OEM module incorporating the chipset necessary to enable a hybrid terrestrial-satellite system in addition to the local LMR would cost the public safety user between $40 and $80 per unit. While this is more than the additional cost of the consumer ATC product, it is substantially less than it would be without the economies of scale resulting from the consumer deployment of ATC. Notably, doing so is cheaper than investing in the software and equipment necessary to achieve interoperability solely by upgrading or replacing existing LMRs.[33] Moreover, achieving interoperability through a flexible architecture (i.e, one that can facilitate ad hoc user groups through shared terrestrial and satellite systems) can be done relatively quickly and cheaply (i.e., compared with SAFECOM's current projections for achieving interoperability[34])—at the same as providing critical redundancy benefits.

[32] Meanwhile, the core radio would continue to have LMR, and could add other capabilities such as the IWIN 162 MHz.

[33] Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (http://commerce.senate.gov/pdf/chiefcarter.pdf) (estimating that improving existing radios to allow interoperability would cost $800 per radio).

[34] The long term vision of SAFECOM foresees achieving interoperability by 2023. See David Boyd, Statement to the Senate Commerce Committee, Session on Communications Interoperability 2 (September 29, 2005) (http://commerce.senate.gov/pdf/boyd.pdf).

Ultimately, the network depicted in Figure 1 (on page 18) would include an overlay for public safety purposes. Significantly, the concept of such a virtual network could be implemented using the same capabilities that mobile virtual network operators (VNO)[35] use today. In order to ensure control, security, and availability, the core network would dedicate resources to the Public Safety VNO, which would operate the public safety serving-network based on applications and policies of its own choosing. The public safety agency would also have the option not only to integrate a multi-mode radio using physically separate modules, but ultimately to use software-defined radios to switch seamlessly between different networks and their associated functionalities.

The vision of using "smart radios" for public safety communications systems would, as Chairman Martin put it, enable them to use "multiple frequencies in multiple formats" and would facilitate a more "flexible infrastructure."[36] As part of such a flexible infrastructure, Chairman Martin emphasized, public safety agencies would incorporate the use of satellite networks, as they "are, in some instances, the most effective means of communicating."[37] Consequently, by using devices like that depicted in Figure 2, public safety agencies could benefit by using a combination of different networks and thereby enjoy (as Figure 1 reflects) a far more impressive footprint and greater level of redundancy than any individual system could offer on its own. Indeed, many public safety agencies recognize the need to incorporate multiple technologies into their system, but are looking for the leadership on what architecture to use as well as financial assistance to upgrade their systems.[38]

---

[35] Mobile Virtual Network Operators (MVNOs) lack network infrastructure or licensed spectrum, but instead use another operator's facilities and capacity to provide an alternative service. In a number of cases, they also possess the back-end systems and enhanced functionalities necessary to provide their service.

[36] Statement of Kevin J. Martin, Hearing on Communications in A Disaster 7 (September 22, 2005). Chairman Martin's observation echoed the findings of an earlier GAO Report. That report explained that "[s]oftware-defined radios will allow interoperability among different agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulations (such as AM or FM)." Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 61-62 (April 2005) (http://www.gao.gov/new.items/d05380.pdf).

[37] *Id.*

[38] Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (http://commerce.senate.gov/pdf/chiefcarter.pdf) (explaining that satellite technology must be a part of a solution that incorporates multiple approaches).

FIGURE 1

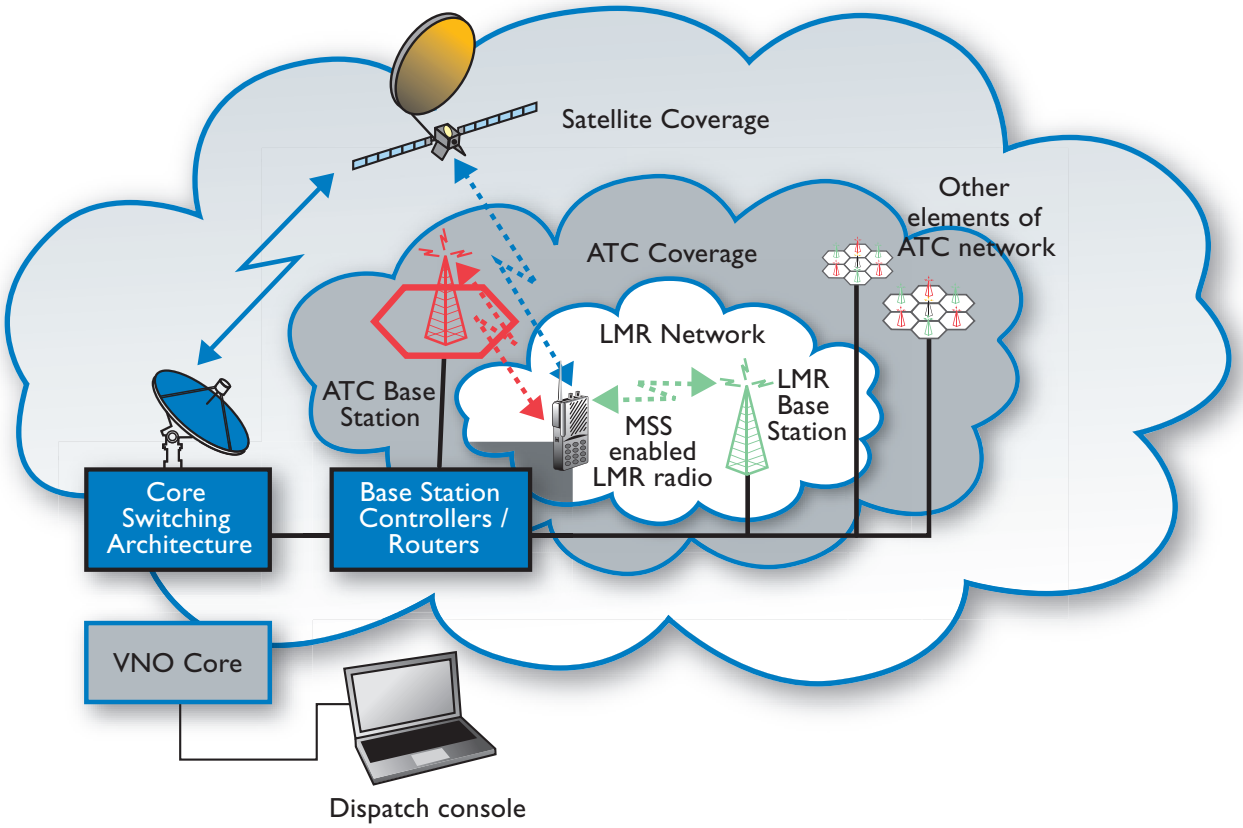
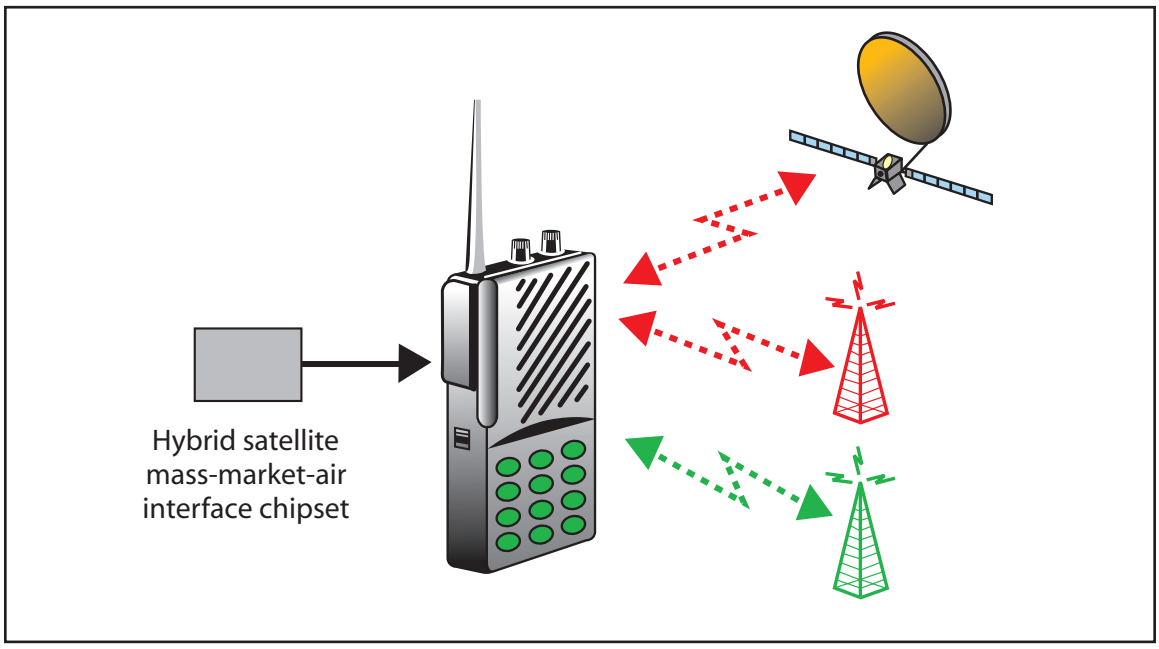


FIGURE 2



NOTE—Both diagrams are conceptual in nature and not drawn to scale

IV. A Policy Strategy For A Next Generation Public Safety Network

The federal government can play a very important role in facilitating the development of an interoperable broadband mobile communications network for public safety agencies. The best strategy, as suggested above, is not necessarily to promote next generation private LMR systems operated by local public safety agencies. Indeed, committing to such a limited vision might well prove problematic on a number of scores (e.g., locking in a costly and potentially inferior technology). Rather, the government should appreciate that the ideal mix between public and commercial networks is one it cannot divine in advance and it should thus promote a hybrid model of public safety networks such as that outlined above. To implement such an approach, we recommend three critical regulatory strategies: (A) making available additional spectrum that can be used for public safety applications by commercial providers; (B) recognizing that a policy of spectrum flexibility benefits public safety agencies by enabling commercial providers to meet their needs; and (C) ensuring that additional appropriations to aid the development of public safety communications promotes the flexible architecture described herein.

A. Making More Spectrum Available for Public Safety Purposes

For quite some time, the discussion over "making available additional spectrum for public safety agencies" has focused on dedicating spectrum for private LMR systems operated by specific agencies. Moreover, this discussion has often centered on the 1996 recommendation by the Public Safety Wireless Advisory Committee that 25 MHz of spectrum was needed by 2001 for public safety purposes, with an additional 72.5 MHz required by 2010. Notably, this recommendation assumes both that (1) achieving interoperability and providing mobile broadband capability will require more spectrum to be specifically dedicated to public safety providers; and that (2) the transition to digital television will be completed in a timely manner so as to free up spectrum for this purpose. Both propositions, however, are far from clear, thereby raising the question of what alternative strategy policymakers might use to enable public safety agencies to migrate toward a next generation network.

Many policymakers continue to take the traditional perspective of focusing on particular spectrum as designated for certain purposes. In the case of public safety, the historical use of spectrum in and around the 700 MHz band makes it understandable that policymakers would focus on whether additional spectrum in this band is necessary to facilitate the transition toward a next generation public safety communications system. But policymakers should be careful not to indulge the two assumptions questioned above—that providing specialized public safety spectrum is necessarily the best policy and that the digital transition will be completed in a manner that will make available such spectrum in a timely fashion. Rather than indulge such assumptions, we urge policymakers to think more broadly about what it means to make more spectrum available for public safety uses.

A broader perspective on the issue would appreciate that the Commission's recent action related to enabling public safety agencies to use spectrum in the 4.9 GHz band for wireless broadband is a form of making additional public safety spectrum available. Thinking even more broadly, it is clear that flexible policies related to SMR spectrum—including its decision to allow Nextel to accumulate dispatch licenses—promoted the development of public safety spectrum, as many public safety agencies now use Nextel's services and benefit from its economies of scale. Similarly, with respect to MSV, the Commission's policies authorizing the use of ATC—as well as its efforts now underway to finalize the distribution of surrendered MSS spectrum in the S Band—promise to make available spectrum that will be commercialized in a manner that will benefit public safety agencies.[39] In addition, in existing MSS bands, such as the L band, it is crucial that the relevant assignments be sensibly configured (e.g., contiguous so as to minimize the needs for guard bands and to support wide-band carriers) so as to ensure efficient use of spectrum and to facilitate broadband applications.

In short, policymakers should appreciate the importance of committing spectrum to commercial providers capable of offering service to public safety agencies. In the case of

[39] The Commission expressly recognized the public safety benefits of ATC in authorizing its use, concluding that "ATC may enhance the nation's overall ability to maintain critical telecommunications infrastructure in times of crisis or disaster." *Flexibility for Delivery of Communications by Mobile Satellite Service Providers in the 2GHz Band, the L-Band, and the 1.6/2.4 GHz Bands*, Report and Order, 18 FCC Rcd 1962, ¶ 29 (February 10, 2003).

satellite providers like MSV, it is not merely sufficient for the FCC to allocate spectrum for use by satellite providers, but it is also critical for it to provide certain and stable assignments of satellite spectrum. Only with such stable assignments, and the ability for providers to undertake significant investments over a period of time, will satellite providers be able to deploy innovative offerings like a hybrid satellite-terrestrial system that will ultimately benefit public safety agencies as well as other consumers.

B. A Policy of Spectrum Flexibility Benefits Public Safety Agencies

It is crucial that policymakers appreciate how promoting spectrum flexibility will greatly benefit public safety agencies. As the Spectrum Policy Task Force Working Group on Spectrum Rights and Responsibilities explained the vices of the old approach:

> From the Commission's experience with command-and-control regulation, it is apparent that overregulation can deter both efficiency and innovation. The highly regulated nature of certain services has tended to discourage technological change because the means of providing permissible services are narrowly defined in terms of current and outdated technology. Moreover, in cases where licensees are limited in what services they are permitted to offer, they have no incentive to seek out a higher valued use for the spectrum.[40]

The Commission's new perspective on spectrum policy takes a fairly critical perspective toward the classic "wise man" restrictions on how spectrum can be used and instead calls for "a light touch and a sense of humility" in developing rules that restrict uses of the spectrum.[41] Thus, as the FCC's Spectrum Policy Task Force concluded, the Commission should look "to increase opportunities for technologically innovative and economically efficient spectrum use, spectrum policy must evolve toward more flexible and market-oriented regulatory models."[42]

---

[40] Federal Communications Commission Spectrum Policy Task Force, *Report of the Spectrum Rights and Responsibilities Working Group* 11 (November 15, 2002) (http://www.fcc.gov/sptf/files/SRRWGFinalReport.pdf).

[41] Jonathan S. Adelstein, *New Frontiers in Wireless Policy: A Framework for Innovation* 3 (April 9, 2003) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-233139A1.pdf).

[42] Federal Communications Commission *Spectrum Policy Task Force, Spectrum Policy Task Force Report* 3, ET Docket No. 02-135 (November 15, 2002).

By reforming its traditional policy toward spectrum management, the Commission will, as Chairman Martin explained, move toward a model of "flexible allocations (that are technology and service-neutral)" of spectrum licenses.[43] This model, which the Commission has begun promoting through initiatives such as its Secondary Markets Order,[44] promises to "create strong incentives for making use of excess capacity" of spectrum already allocated in inflexible ways.[45] Significantly, by continuing to make progress on spectrum reform more generally, policymakers can assist public safety agencies in particular by helping to make the network architecture outlined above more effective and less expensive.

C. Funding For Public Safety Agencies Should Promote A Flexible Architecture

For many public safety agencies, their first priority and instinctive response is to replace their old equipment with expensive, often proprietary, and single-use systems. In many respects, public safety agencies' attachment to LMRs of the kind that have served them relatively well is readily understandable—after all, familiarity often leads to comfort. In the case of technology products like mobile radios, however, public safety agencies should appreciate that (1) multi-mode radios; (2) economies of scale from off-the-shelf and commercially provided products; and (3) the opportunity to incorporate satellite backup into their systems are all opportunities that cannot be ignored. To facilitate greater understanding of such issues and to help develop the relevant technology, policymakers should consider funding both development of prototype models and demonstration projects as well as to fund greater research into the development and deployment of advanced technologies.

In providing important leadership on this issue, the federal and state governments should not allow local purchasing agents to act on auto-pilot and miss the option to migrate to a flexible,

---

[43] Kevin J. Martin, U.S. *Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html).

[44] *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order, 18 FCC Rcd 20,604 (2003).

[45] Kevin J. Martin, U.S. *Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html).

next generation architecture. By using its power of purse thoughtfully, the federal government can play an incredible important role in this regard. Most important of all, policymakers should avoid requiring or creating incentives that would have the effect of foreclosing the type of architecture embraced by this White Paper.

CONCLUSION

To learn from what went right and wrong in the aftermath of Hurricane Katrina, policymakers should avoid the impulse to assume that simply granting more spectrum for public safety agencies and appropriating more money to invest in LMRs will solve the problems of public safety communications. Rather, both policymakers and the public safety agencies themselves should look beyond this traditional mindset and develop a next generation architecture that would incorporate satellite, terrestrial, and emerging wireless broadband networks into a single seamless system. To promote this system, policymakers should focus on making spectrum *generally* available for broadband uses, whether via unlicensed WiFi-like systems, licensed commercial carriers, or satellite providers (including those using hybrid satellite-terrestrial networks with the aid of ATC technology) and ensuring that any government funding promotes a flexible architecture for public safety communications. By so doing, policymakers can best advance a next generation public safety communications strategy that can provide a reliable, survivable, and secure network for all first responders.

Particularly in light of the lessons underscored by Hurricane Katrina, adhering to the traditional model of relying solely on LMRs is no longer sustainable and policymakers must consider a more flexible and robust next generation architecture for public safety communications. Significantly, such a system would facilitate the greater use of satellite technology, such as was used effectively in New Orleans and the Gulf Coast in the wake of Katrina, and would embrace the use of hybrid satellite-terrestrial systems. In so doing, policymakers would make available far more cost-effective access to satellite technology than today's satellite terminals and ensure that users of this technology only used the satellite capacity when it is truly needed. And most importantly, such networks would switch seamlessly between available networks to enable first responders to use a single handset and not worry about what network is optimal; instead, the device would automatically select the appropriate network.

By implementing effective spectrum policies, encouraging the developing of hybrid solutions, and funding the purchase of more technically advanced solutions (e.g., multi-mode radios that include satellite and other technologies), policymakers can advance a next generation public safety network strategy. Notably, by promoting a public safety network where agencies can use spectrum licensed to commercial providers, available in unlicensed bands as well as dedicated to their private LMRs, public safety agencies will gain the benefits of a modern, innovation-rich, low cost network. In particular, public safety agencies will benefit from modular, extensible networks that can take advantage of cutting edge applications that ride on their private LMR, a commercially provided, or an unlicensed wireless broadband network. If, by contrast, policymakers focus exclusively on supporting single purpose LMR equipment and dedicated spectrum (say, in the 700 MHz band), they risk pursuing an antiquated technological architecture that will continue to leave public safety agencies without the best available tools for interoperable, reliable, secure, and broadband communications.

DALE HATFIELD is an Adjunct Professor of Telecommunications at the University of Colorado and an internationally recognized expert, teacher, and consultant on telecommunications technology and policy. Over his distinguished career in both the public and private sector, he founded a very successful consulting firm and served as the Federal Communications Commission's Chief of the Office of Engineering and Technology, Chief Technologist, and Chief of the Office of Plans & Policy. Professor Hatfield's many honors include: a Department of Commerce Silver Medal for contributions to domestic communications satellite policy, the Attorney General's Distinguished Service Award and the FCC's Gold Medal Award for distinguished service.

PHIL WEISER is an Associate Professor of Law and Telecommunications at the University of Colorado and the Founder and Executive Director of the Silicon Flatirons Telecommunications Program. After graduating from New York University School of Law, Professor Weiser served as a law clerk to the Tenth Circuit Court of Appeals Judge David M. Ebel and to United States Supreme Court Justices Byron R. White and Ruth Bader Ginsburg. Before taking his position at CU, Professor Weiser served as the Senior Counsel for Telecommunications Policy to Joel Klein, Assistant Attorney General, Antitrust Division, at the U.S. Department of Justice. Professor Weiser teaches and writes widely on information policy issues and is the author (with Jon Nuechterlein) of "Digital Crossroads: American Telecommunications Policy In the Internet Age (MIT Press 2005)."

For additional copies please contact:

Mobile Satellite Ventures

whitepapers@msvlp.com